

ORIGIN DS-00

INFO	LOG-00	MFA-00	EEB-00	AF-00	AIT-00	A-00	CIAE-00
	INL-00	DNI-00	DODE-00	DOEE-00	WHA-00	EAP-00	DHSE-00
	EUR-00	OIGO-00	OBO-00	TEDE-00	INR-00	IO-00	JUSE-00
	LAB-01	L-00	MMP-00	MOFM-00	MOF-00	NEA-00	DCP-00
	ISN-00	NSCE-00	NSF-01	OES-00	OIG-00	P-00	ISNE-00
	DOHS-00	FMPC-00	SP-00	IRM-00	SSO-00	SS-00	DPM-00
	USSS-00	NCTC-00	CBP-00	DSCC-00	PRM-00	DRL-00	SCA-00
	SAS-00	FA-00	/002R				

P 031812Z NOV 08
FM SECSTATE WASHDC
TO SECURITY OFFICER COLLECTIVE PRIORITY
AMEMBASSY TRIPOLI PRIORITY
INFO AMCONSUL CASABLANCA PRIORITY
XMT AMCONSUL JOHANNESBURG
AMCONSUL JOHANNESBURG

S E C R E T STATE 116943

NOFORN

E.O. 12958: DECL: MR
TAGS: [ASEC](#)
SUBJECT: DIPLOMATIC SECURITY DAILY

Classified By: Derived from Multiple Sources

SECRET//FGI//NOFORN//MR
Declassify on: Source marked 25X1-human, Date of source:
October 30, 2008

1. (U) Diplomatic Security Daily, November 1-3, 2008
2. (U) Significant Events) Paragraphs 7-13
3. (U) Key Concerns) Paragraphs 14-18
4. (U) Threats & Analysis) Paragraphs 19-31
5. (U) Cyber Threats) Paragraphs 32-45
6. (U) Suspicious Activity Incidents) Paragraphs 46-49
7. (U) Significant Events
8. (SBU) EUR - Ireland - Emergency Action Committee (EAC)
Belfast met October 31 to discuss the armed forces homecoming parade scheduled for November 2 and the planned simultaneous counter-demonstrations by Sinn Fein and the dissident republican group Eirigi. Discussions centered on the parade route and the possibility of confrontations and violence in different areas, as well as the presence of AmCits along the parade and demonstration routes. The EAC decided the U.S. Consulate General should release a Warden Message to warn AmCits in Belfast. (Belfast 0137)
9. (SBU) Sweden - Approximately 12 to 15 protesters, carrying banners and flags requesting fair treatment for the Cuban Five8 in Guantanamo Bay, Cuba, made an unscheduled appearance at U.S. Embassy Stockholm November 1. The group emerged from the nearby German Embassy and stopped briefly in front of Post. The RSO monitored the group; they did not attempt to contact Embassy officials, but appeared more interested in photographing the front of Post. The protesters departed within a few minutes before Embassy police could respond. No damages or injuries were reported. (RSO Stockholm Spot Report)
10. (S//NF) NEA - Egypt - EAC Cairo convened October 20 to review recent threat reporting and assess any threats specific to the planned visit by U.S. Secretary of State Condoleezza Rice on November 8 and 9. The EAC agreed there is no new, specific, and/or credible threat to U.S. interests in Egypt, but also assessed that Egypt remains a very tempting target for both indigenous and transnational terrorist elements. EAC members also agreed to enhance security

measures at the American Presence Post in Alexandria. The EAC continues to assess the Government of Egypt,s (GoE) counterterrorism efforts as effective, and Post has a close relationship with the GoE on security matters. (Appendix 1)

¶11. (S//NF) Kuwait - EAC Kuwait City convened November 2 to discuss the security impact of recent threat reporting, Embassy Kuwait election coverage, U.S. Marine Corps Birthday Ball, and the upcoming visit of the former U.S. President William J. Clinton. The EAC was briefed on the recent reporting of possible terrorist surveillance of housing areas within Kuwait City. Post is coordinating the release of this information to the Kuwait Security Service for further action. The RSO stated the Local Guard Force (LGF) Mobile Patrol unit will increase coverage in the housing occupied by Chief of Mission personnel within the named areas, defensive counterintelligence training will be given to locally employed staff, and a Security Notice reminding personnel to remain vigilant in their personal security procedures will be released. The EAC concluded that Post,s current security posture is appropriate for the planned events. (Appendix 2)

¶12. (S//NF) EAP - Indonesia - EAC Jakarta convened October 30 to discuss the security implications of the anticipated execution of the Bali bombers. The Government of Indonesia (GoI) recently announced they would be executed during the first week of November. Rumors are circulating around Jakarta that retaliatory attacks and demonstrations by those who support the bombers are possible. However, there is no specific or credible information regarding the planning of these types of attacks. One report mentioned possible suicide bomber attacks on shopping malls in Jakarta, specifically the Kelapa Gading mall in northern Jakarta, but without details. The U.S. Embassy assesses the likelihood of a terrorist attack conducted against U.S. or other Western interests in direct response to the executions is low. (Appendix source 3)

¶13. (SBU) SCA - Pakistan - A motorcade carrying Pakistani Deputy Inspector General of Police Syed Akhtar Ali Shah was targeted by a suicide vehicle-borne improvised explosive device (IED) attack in Mardan Province on October 31 at around 2:30 p.m. Ali Shah and 20 others were wounded, and nine police officers were killed in the attack. On November 1, at approximately 2:33 a.m., an explosion occurred at a police substation approximately 2,000 meters from the U.S. Consulate Peshawar residential area and official annexes. One police officer was killed and several other individuals were badly wounded. It is undetermined at this time whether the explosion was from a rocket or an explosion charge placed at the structure. The RSO will monitor these attacks. (RSO Peshawar Spot Report)

¶14. (U) Key Concerns

¶15. (S//FGI//NF) NEA - Lebanon - Al-Qa,ida affiliate to attack U.S. Embassy motorcade: According to a source of the Jordanian General Intelligence Directorate, as of mid-October, al-Qa,ida-affiliated elements in the Ayn al-Hilwah Palestinian refugee camp plan to attack a U.S. Embassy motorcade in Beirut. The men planning the operation had already collected an unspecified amount of explosives and a white 1983 Mercedes, which was currently inside the Shatila Palestinian refugee camp. The Mercedes was to be rigged with the explosives. (Appendix source 4)

¶16. (S//FGI//NF) SCA - Maldives - Continued monitoring of al-Qa,ida associates: The Maldives Police Service continued to investigate and monitor the activities of Maldives-based al-Qa,ida associates Yoosuf Izadhy, Easa Ali, and Hasnain Abdullah Hameedh (a.k.a. Hameed). Izadhy was reportedly in contact with a militant group in Waziristan, which allegedly maintained unspecified links to al-Qa,ida. Izadhy was clandestinely working to recruit others into his organization, specifically seeking individuals who had undergone basic terrorism training in Pakistan. Izadhy planned to create a terrorist group in the Maldives with the assistance of the Waziristan-based group. Izadhy planned to send his members to Waziristan for training. Hameedh was in

close contact with a number of individuals who had undergone training in Pakistan, including individuals who were members of Jamaat-ul Muslimeen and completed basic and advanced training by Lashkar-e-Tayyiba (LT) in Pakistan. They followed the ideology of Abu Easa.

¶17. (S//FGI//NF) DS/TIA/ITA notes, while the operational aspirations of Yoosuf Izadhy (Terrorist Identities Datamart Environment (TIDE) number 17312323), Easa Ali (TIDE number 17312652), and Hasnain Abdullah Hameedh (TIDE number 20686145) are unclear; past reporting suggests Maldivian extremists have demonstrated interest in actively participating in global jihadi activities by attempting to arrange travel and terrorist training in Pakistan. While many Maldivian participants of extremist online forums aimed to ultimately fight Coalition forces in Iraq and Afghanistan, mid-October 2007 debrief information following the September 29 bombing in Male that targeted tourists indicates at least two of the operatives participated in the attack in exchange for travel from the islands after the operation and arranged study at a madrassa in Pakistan.

¶18. (S//NF) Specific links to al-Qa,ida remain unclear; although, reporting from May detailed recruitment activity by Maldivian national Ahmed Zaki of Maldivians into the Kashmiri extremist group LT madrassas and training camps in Pakistan. A variety of reports from 2006 details linkages between Maldivians belonging to a group known as Jama-ah-tul-Muslimeen (JTM) and individuals participating in an anti-American Islamic extremist online forum called Tibyan Publications. JTM is an extremist group based in the UK that follows an extremist ideology known as Takfiir that actively encourages violent jihad and supports criminality against apostate states. (Appendix sources 5-18)

¶19. (U) Threats & Analysis

¶20. (S//NF) WHA - Mexico - Violence spikes again in Tijuana: According to a mid-level Baja California state police official, a turf war between the Arellano Felix Organization (AFO) and the Sinaloa Cartel has caused another increase in violence in Tijuana. The Mexican Government,s counternarcotics efforts -- in the form of 3,300 military and police assets patrolling the area under Operation Tijuana -- have severely weakened the AFO,s operations. The Sinaloa Cartel, hoping to capitalize on the AFO,s weaknesses, is battling for control of Tijuana,s drug plaza. While the AFO assassins are skilled, Sinaloa Cartel hit men are poorly trained and have no aversion to public shootings; however, if the Sinaloa Cartel successfully ousts the AFO from Tijuana, DS/TIA/ITA notes the levels of violence should decrease. While residents and visitors are not being targeted, the likelihood of being in the wrong place at the wrong time is of increasing concern. Cartel targets are being killed during daytime hours in public areas of Tijuana, including restaurants, shopping centers, and near school buildings. The DoS, Travel Alert for Mexico was extended for six months on October 14 to reflect the current and widely reported crime and violence occurring throughout Mexico. (Open sources; Appendix sources 19-20)

¶21. (U) AF - Cameroon - An examination of the background, goals, and tactics of the Niger Delta Defense and Security Council and the Bakassi Freedom Fighters: (S//NF) The October 31 kidnapping of approximately 10 hostages off the shores of the Bakassi Peninsula has magnified the role of two groups -- the Bakassi Freedom Fighters (BFF) and the Niger Delta Defense and Security Council (NDDSC) -- in the increasing insecurity in the Bakassi. The kidnappings, an overview of the NDDSC,s and BFF,s background, and an examination of their past operations, highlight the groups, possible intent to use novel, deadly, and unprecedented tactics to achieve their goals.

¶22. (SBU) In the early morning of October 31, a group of armed men in three boats attacked a French Total vessel named Bourbon Sagita, which was located off the Cameroonian shore between Bakassi and Limbe. Although no Americans were

directly impacted, at least seven French citizens, one Tunisian, one Senegalese, and several Cameroonian nationals were kidnapped; five remaining oil workers were left on the boat. Nobody was injured in the attack.

¶23. (SBU) According to unconfirmed media reports, shortly after the raid, the BFF, part of a larger and shadowy alliance of the NDDSC, claimed responsibility for the attacks and threatened to kill the hostages, stating, &The 10 are in our hands. If you don,t tell the government of Cameroon to come here and discuss with us, we will kill them all in three days.8 On November 1, the NDDSC/BFF withdrew the threat, but stated it would hold the hostages until the government opened negotiations with them.

¶24. (S//NF) The NDDSC/BFF is likely referring to discussions over the status of the Bakassi Peninsula in its statement. The region was transferred from Nigeria to Cameroon on August 14, per an International Court of Justice ruling. According to e-mails it sent to media outlets, the NDDSC/BFF merged into an official alliance at the end of July in an attempt to forestall the hand over. Led by Commander Ebi Dari and General A.G. Dasuo, who claim they are fighting for &self-determination and freedom8 of the Bakassi Peninsula which contains a majority of Nigerian citizens. They are also demanding that two of their fighters captured in July be released and that Nigerians on the Bakassi Peninsula be compensated.

¶25. (S//NF) An intelligence and open media search of the BFF provided negligible results. Meanwhile, although little background information is known about the NDDSC, it claims to have approximately 1,050 fighters. It has been in existence since at least 2002 and previously conducted low-level attacks against Cameroonian troops on the Bakassi. It can also be linked to three deadly operations prior to the hand over of the controversial region. In the most macabre raid, on June 9, the NDDSC allegedly killed and mutilated six members of a Cameroonian delegation visiting the Peninsula, including the deputy subregional commander. It also claimed responsibility for a November 2007 raid on a Cameroonian military outpost which killed 21 soldiers; this claim remains unconfirmed. (Please see the July 26 DS Daily for further information on the pre-hand over security incidents in the Bakassi.)

¶26. (S//NF) Although the post-hand over period has been defined by a series of attacks, the NDDSC/BFF has released statements denying culpability in some of those operations. These include a September 28 bank robbery in Limbe and a September 13 attack against a trawler off the Bakassi Peninsula. The NDDSC/BFF may be responsible for some post-hand over operations, while others may have been conducted by different militants in the region, including in the Niger Delta. Despite similar tactics in all these operations, including the use of speedboats carrying heavily armed masked men, at this time, there are no clear indications the NDDSC/BFF has a defined relationship with the Movement for the Emancipation of the Niger Delta (MEND) or any other prominent Niger Delta group.

¶27. (S//NF) Instead, the series of raids by the NDDSC/BFF may possibly signify new tactics being pursued in the Bakassi region. In its early raids, the NDDSC/BFF primarily used deadly and brutal force against the Cameroonian military, but often spared expatriates and civilians. Two recent attacks, however -- the June 9 attack and the October 31 hostage-taking operation -- have demonstrated its desire to expand its targets. In the June 6 raid, the NDDSC targeted a political delegation and mutilated a deputy subregional commander, the equivalent of a governor. It is unclear if the NDDSC was directly targeting the governor; but, nevertheless, the group demonstrated its desire to also kill politicians. For its part, the October 31 attacks was the first kidnapping of expatriates off the coast of Cameroon.

¶28. (S//NF) Also of concern is the NDDSC/BFF,s intent to hold hostages indefinitely after initially threatening to

kill them. Whereas MEND and other Delta groups kidnapped hostages primarily to garner ransom money or to force oil companies to scale back operations, they had seldom directly harmed or threatened to kill hostages. They also often released hostages shortly after their capture. Moreover, given its intent to hold the hostages for a political objective, the NDDSC/BFF may find it convenient to continue operations against expatriates in the region to pressure the Cameroonian Government and to ensure that its political demands are met. (Open sources; Yaound 1071; 0754; 0706; Appendix sources 21-28)

¶29. (S//FGI//NF) SCA - Bangladesh - Rejection of IDP to register for December elections: As of late October, the Bangladeshi Election Commission was set to reject the Islamic Democratic Party,s (IDP,s) attempt to register for the December parliamentary elections. The IDP is a nascent political party formed by senior members of the Islamic terrorist group Harakat-ul-Jihad-i-Islami Bangladesh (HUJI-B). Bangladesh,s Directorate General of Forces Intelligence (DGFI) supported the formation of the IDP as a way to bring HUJI-B into the mainstream and reported it tightly monitored the group,s activities; although, HUJI-B has never renounced the use of violence to implement its vision of transforming Bangladesh into a Muslim theocracy. According to U.S. Embassy Dhaka, which strongly opposed the creation of the IDP, the party and its leadership will likely be angered by the decision and may respond with violence possibly against the commission or the U.S. Mission or interests.

¶30. (S//NF) Arrests and monitoring have undoubtedly hindered HUJI-B,s capabilities in recent years, and it is entirely plausible the group is pursuing the creation of a political wing to improve its ability to support and carry out terrorist activity. A late-September assessment from Bangladesh,s National Security Intelligence Organization (NSI) voiced concern that the party,s creation would free extremists to pursue extremist activity under the cover of a moderate front organization. Indeed, there are no indications IDP would garner a significant number of votes. Analysis from the DoS, Office of Research noted the majority of Bangladeshis want Awami League and Bangladesh National Party leaders Sheikh Hasina and Khaleda Zia to participate in the December elections. Interestingly, 80 percent stated they would ignore a call by either party to boycott the vote. One-third further stated they would join street protests in the face of a cancellation of elections.

¶31. (S//FGI//NF) Although there is little information available regarding HUJI-B,s current capabilities, its membership likely does retain the ability to manufacture and use explosives and has previously favored targeting high-profile individuals for attack. While there is no specific reporting at the present time detailing plots against U.S. interests in Bangladesh, the group has publicly articulated its anti-Western and -Indian stance, including signing Usama Bin Ladin,s 1998 fatwa against the West. In regards to HUJI-B,s capabilities, DGFI,s, Rapid Action Battalion,s (RAB,s), and NSI,s assessments vary significantly. Following the early-March U.S. designation of HUJI-B as a foreign terrorist organization, RAB assessed HUJI-B would not respond with violence due to the severe degradation of the group,s capability and leadership structure from arrests and active surveillance. Some member who wanted to independently attack Western interests, however, remained technically capable of carrying out low-level attacks using small arms, grenades, and IEDs. DGFI likewise reported HUJI-B was &an organization on the run8 and that it did not pose a threat to U.S. interests in Bangladesh. NSI conversely assessed HUJI-B would react violently to the designation and would attempt to conduct an attack against the U.S. official presence in Dhaka; although, there was no information available detailing such an operation. Thus far, HUJI-B has not carried out an attack against American interests in Bangladesh, but the group has been linked to assassination attempts on intellectuals, journalists, and politicians, including two thwarted attempts

on the life of Prime Minister Sheikh Hasina during public addresses and a grenade attack that injured the British high commissioner in May 2004. (&Bangladeshis have high hopes for national elections,8 DoS Office of Research; Appendix sources 29-40)

¶32. (U) Cyber Threats

¶33. (S//REL TO USA, FVEY) WHA - CTAD comment: On October 16, at least one e-mail account within the Government of Canada received a Trojanized message from a Yahoo account claiming to represent a U.S. embassy. The bogus subject line was an invitation for a private meeting with a named DoS employee. The attached Microsoft Word document was a malicious &invitation8 file that, when opened, attempts to beacon and create a connection to &jingl.cable.nu8 via port 8080. The &cable.nu8 domain remains one of concern, as it has historically been associated with activity from Chinese hacker organizations.

¶34. (U) EUR - CTAD comment: The European Commission (EC) this week proposed legislation to establish a Critical Infrastructure Warning Information Network (CIWIN) to improve information sharing among European Union (EU) member nations. The proposed legislation would enable the EC to launch and manage the CIWIN, a secure information technology (IT) system aimed at sharing knowledge on threats, vulnerabilities, and protection of critical infrastructures. The CIWIN would be a voluntary tool for transmitting sensitive information and would also include a rapid alert system for critical infrastructure, allowing EU nations to post alerts on immediate threats.

¶35. (U) AF - CTAD comment: Sudanese law enforcement recently reported the arrest of three hackers who have allegedly attacked more than 300 government and public websites during the last few months. Among the hacked sites was that of the National Telecommunication Corporation, which is responsible for oversight of telecommunication service providers as well as many other aspects of Sudanese IT and network stability. The three highly skilled hackers, all of whom are Sudanese, reportedly caused significant damage to their targets, but their motivation for the attacks and any potential group affiliations are yet undetermined.

¶36. (C) NEA - CTAD comment: On October 21, officials from the Kuwaiti Central Agency for Information (CAIT) and the National Security Bureau (NSB) expressed concerns for foreign and domestic threats to Kuwaiti information systems. According to these organizations, some of the issues plaguing Government of Kuwait (GoK) networks are suspected attacks from Iranian hackers, insider corruption and misuse of resources, and a lack of sufficient interagency coordination and guidance for monitoring users, activities and investigating incidents. For example, the groups, inability to adequately examine malicious software (malware) injections or internal abuse of system access continues to hinder the GoK,s capacity to ensure the protection of sensitive information. Therefore, the CAIT and NSB are interested in learning more about U.S. cyber security programs as well as receiving additional training and support.

¶37. (S//NF) EAP - CTAD comment: Between September 29 and October 2, a conference was held by the German Federal Office for the Protection of the Constitution (BfV). During this conference, the BfV delivered a briefing on its analysis of the cyber threat posed by the People,s Republic of China (PRC), which appears to mirror conclusions drawn by the U.S. Intelligence Community. The BfV surmises the intention of PRC actors is espionage, and the primary attack vector used in their malicious activity is socially engineered e-mail messages containing malware attachments and/or embedded links to hostile websites. According to reporting, &from October 2006 to October 2007, 500 such e-mail operations were conducted against a wide range of German organizations,8 and the attacks appear to be increasing in scope and sophistication. The socially engineered e-mail messages delivered to German computer systems were spoofed to appear

to come from trusted sources and contain information &targeted specifically to the recipient,s interests, duties, or current events.⁸ This malicious activity has targeted a wide variety of German organizational levels to include &German military, economic, science and technology, commercial, diplomatic, research and development, as well as high-level government (ministry and chancellery) systems.⁸ In addition, German intelligence reporting indicates an increase in activity was detected immediately preceding events such as German Government, or commercial, negotiations involving Chinese interests.

¶38. (U) SCA - CTAD comment: The National Science Foundation and the Pakistan Higher Education Commission recently announced the establishment of a Pakistan extension to an international high-speed network already connecting U.S. and EC systems. The new portion of the network links Pakistani scientists and students to facilities in the U.S. through additional connections to Singapore and Japan. This project emerged from February 2007 discussions of the U.S.-Pakistan Joint Committee on Science and Technology that sought to promote cooperation and innovation among education and business sectors. (Open sources; Appendix sources 41-43)

¶39. (S//NF) Worldwide - BC conducting CNE on USG systems:

¶40. (S//NF) Key highlights:

BC actively targets USG and other organizations via socially engineered e-mail messages.
BC actors recently compromised the systems of a U.S. ISP to carry out CNE on a USG network.
Additional IP addresses were identified this month as compromised and used for BC activity.
BC has targeted DoS networks in the past and may again in the future via spoofed e-mail.

¶41. (S//REL TO USA, FVEY) Source paragraph: &Byzantine Candor (BC) actors have compromised multiple systems located at a U.S. Internet service provider (ISP) and have used the systems as part of BC,s U.S.-based attack infrastructure since at least March, targeting multiple victims including at least one USG agency.⁸

¶42. (S//NF) CTAD comment: Since late 2002, USG organizations have been targeted with social-engineering online attacks by BC actors. BC, an intrusion subset of Byzantine Hades activity, is a series of related computer network intrusions affecting U.S. and foreign systems and is believed to originate from the PRC. BC intruders have relied on techniques including exploiting Windows system vulnerabilities and stealing login credentials to gain access to hundreds of USG and cleared defense contractor systems over the years. In the U.S., the majority of the systems BC actors have targeted belong to the U.S. Army, but targets also include other DoD services as well as DoS, Department of Energy, additional USG entities, and commercial systems and networks. BC actors typically gain initial access with the use of highly targeted socially engineered e-mail messages, which fool recipients into inadvertently compromising their systems. The intruders then install malware such as customized keystroke-logging software and command-and-control (C&C) utilities onto the compromised systems and exfiltrate massive amounts of sensitive data from the networks. This month, BC actors attempted to compromise the network of a U.S. political organization via socially engineered e-mail messages (see CTAD Daily Read File dated October 16).

¶43. (S//REL TO USA, ACGU) CTAD comment: Also discovered this month by USG analysts was the compromise of several computer systems located at a commercial ISP within the United States. According to Air Force Office of Special Investigations (AFOSI) reporting, hackers based in Shanghai and linked to the PRC,s People,s Liberation Army (PLA) Third Department have been using these compromised systems as part of the larger BC attack infrastructure to facilitate computer network exploitation (CNE) of U.S. and foreign information systems. Since March, the responsible actors have used at least three separate systems at the unnamed ISP in multiple

network intrusions and have exfiltrated data via these systems, including data from at least one USG agency. AFOSI reporting indicates, on March 11, BC actors gained access to one system at the ISP, onto which the actors transferred multiple files, including several C&C tools. From here, the intruders used the tools to obtain a list of usernames and password hashes for the system. Next, on April 22, BC actors accessed a second system at the ISP, where they transferred additional software tools. From April through October 13, the BC actors used this computer system to conduct CNE on multiple victims. During this time period, the actors exfiltrated at least 50 megabytes of e-mail messages and attached documents, as well as a complete list of usernames and passwords from an unspecified USG agency. Additionally, multiple files were transferred to the compromised ISP system from other BC-associated systems that have been previously identified collecting e-mail messages from additional victims. The third system at the U.S. ISP was identified as compromised on August 14, when BC actors transferred a malicious file onto it named &salaryincrease-surveyandforecast.zip.8 According to AFOSI analysis, BC actors use this system to host multiple webpages that allow other BC-compromised systems to download malicious files or be redirected to BC C&C servers.

¶44. (S//REL TO USA, FVEY) CTAD comment: Additional DoD reporting this month indicates BC actors have used multiple other systems to conduct CNE against U.S. and foreign systems from February through September. A October 23 DoD cable states Shanghai-based hackers associated with BC activity and linked to the PLA have successfully targeted multiple U.S. entities during this time period. The cable details dozens of identified Internet Protocol (IP) addresses associated with BC activity as well as the dates of their activity. All of the IP addresses listed resolve to the CNC Group Shanghai Province Network in Shanghai, and all the host names of the addresses contained Asian keyboard settings as well as China time zone settings. Most of these IP addresses were identified as responsible for direct CNE of U.S. entities, including unspecified USG organizations, systems and networks. Interestingly, although the actors using each IP address practiced some degree of operational security to obfuscate their identities, one particular actor was identified as lacking in these security measures. On June 7, the BC actor, using an identified IP address, was observed using a Taiwan-based online bulletin board service for personal use.

¶45. (S//NF) CTAD comment: BC actors have targeted the DoS in the past on multiple occasions with socially engineered e-mail messages containing malicious attached files and have successfully exfiltrated sensitive information from DoS unclassified networks. As such, it is possible these actors will attempt to compromise DoS networks in the future. As BC activity continues across the DoD and U.S., DoS personnel should practice conscientious Internet and e-mail use and should remain informed on BH activity. (Appendix sources 44-46)

¶46. (U) Suspicious Activity Incidents

¶47. (SBU) EUR - Azerbaijan - A vehicle with Iranian license plates was parked adjacent to U.S. Embassy Baku October 29. The driver was the only occupant in the car. Another subject appeared and got into the car, which then took off. The police have been asked to check the vehicle registration. Post is awaiting the results. (SIMAS Event: Baku-00507-2008)

¶48. (SBU) EAP - Taiwan - An Asian male with a professional video camera stood across the street from the American Institute in Taiwan (AIT) October 29. He filmed a number of buildings in the area and possibly the AIT. After a few minutes, the subject departed the area on a motor scooter. (SIMAS Event: Taipei-00194-2008)

¶49. (SBU) Taiwan - An Asian male stood in front of the Bank of Taiwan and photographed various buildings -- including the AIT -- on October 31. An LGF member stopped and questioned

the man, who refused to show identification or the pictures he took. He left the area on foot shortly afterward. (SIMAS Event: Taipei-00195-2008)

SECRET//FGI//NOFORN//MR

Full Appendix with sourcing available upon request.

RICE